HQDA G-2 Special Security Office

The Guardian

" Serving the Army's Warfighters"

In This Issue

References

DOD 5105.21-M-1

DCID 6/9

Contact Us

http://www.dami.army.pentagon.mil/dami-cd/sso/index

Our Location

Room 1A272

The Pentagon

A Message from Our SSO:

Greetings fellow security officials! Welcome to our first production of "The Guardian". This newsletter and those to follow will provide operational and policy updates that can be used by all security professionals. The newsletter will also convey any areas of concerns that we have noticed during daily operations.

Over the past several months, the Special Security Office (SSO) has experienced several changes. As you may know, we are transitioning from military to civilian positions. We are a few months away from completion and you should not notice any disruption in operations. In the near future, we will ramp up our Staff Assistant Visit program. In the past we primarily inspected the area of Physical Security. We are going to expand that to include all Sensitive Compartmented Information (SCI) Security Functions, specifically in the areas of Personnel and Information Security. Please check out our websites (NIPRNET, SIPRNET and JWICS) and I encourage your feedback and input to help us improve our operations.

I would like to take this opportunity to say farewell to some outstanding Soldiers; SFC Johnson-Robinson, SFC Johnson, SSG Kelly-Jones, and SSG Louis. They provided excellent service while they were here and will truly be missed. SSG Krogel is no longer in the Pentagon Office, however, he has moved to Raven Rock to work with Mrs. Keister.

I would like to welcome our newest additions to the office, Mr. James Davis and Mrs. Trina Gooden. James will provide service in Personnel Security while Trina will perform duties as the Information Security Specialist. She is also responsible for our website and Security Education and Awareness Training.

Please enjoy the newsletter and provide me feedback on articles you would like to see in the future or if you would like to be a guest author. Thanks, and have a great spring!! **LTC Carroll**

Personnel Security on Foreign Travel

TRAVELING OR VISITING FOREIGN COUNTRIES ON OFFICIAL OR PERSONAL TRAVEL?
You may have reporting requirements!

While summer marches towards us, many of us are sitting in the office cubicle looking for the nearest escape and dreaming of a place far, far away, from the long commutes on the beltway, maybe even dreaming of exploring tropical beaches in a foreign land. Or, maybe you have to travel to a foreign country on TDY. Whatever the case, the urge or requirement to travel to foreign soil may be hitting a lot of personnel who are read on to SCI. But before you rush off to the airport with luggage in tow, there are several important requirements that you have to complete, which are stated in the Department of Defense (DoD) SCI Administrative Security Manual, dated August 1998, DoD 5105.21-M-1 Chapter 2, Paragraphs R and S:

1. All personnel that are read on to SCI are required to report all foreign travel to their Supervisor or SSO.
2. Obtain a foreign travel briefing from your SSO, this can be a written briefing or the video, "Expect the Unexpected, Defense Tactics for a Safe Trip Abroad," put out by the Defense Intelligence Agency (DIA), dated December 2000.
3. Report any contacts with foreign nationals that are of a personal or unfriendly nature to your immediate supervisor or SCI security official within 72 hours.

Despite how familiar you may be with a country, you should never let your guard down and you should always expect the unexpected. As an employee of DoD or other government agency, you are an ideal target of opportunity for foreign intelligence, terrorists, and criminals.

Foreign Intelligence
To protect the grave danger to our National Security, SCI-indoctrinated personnel must protect themselves against cultivation and possible exploitation by foreign nationals who are or may be working for foreign intelligence services and to whom they might unwittingly provide sensitive or classified national security information. Due to the increase of technology, Foreign Intelligence can be collected in more methods than previously shown in the James Bond 007 films. Today's foreign intelligence is collected via: traffic cameras, foot and vehicle surveillance, observation posts or lookouts, and video and audio recording. Think of how easy it is to take a

picture from your cell phone nowadays and that will give you a good idea of how easy it is to gather intelligence against you. Do not attempt to photograph or search for monitoring devices. The host country may think you have something to hide and detain you for information. Always assume you are under surveillance!

Terrorists / War / Civil Disturbance
Since 9/11, the reach of terrorism has stretched to every corner of the world and many countries lay on a fine line between peace and civil disturbance, especially in the Middle East, Europe, and the Balkans. In order to reduce your risk of being caught in the middle of such events, take the following steps: avoid large gatherings, be mentally prepared, orient yourself with several escape exits, know the phone numbers to the nearest U.S. Embassy and or Consulate, 24 hour United States Marine Corps Security Guard, and your Conus Point of Contact. If a situation does arise, alert the U.S. Embassy and or Consulate of your location and take cover until help arrives.

Crime
In many countries, what you carry in your wallet equals what they might make in 2-3 years of their wages and therefore you are considered rich and a high priority, ideal target of opportunity. The key to not becoming a target is to keep a low profile and be prepared for anything that can happen. Here are some very helpful tips to practice while traveling overseas:

Prior to traveling, educate yourself on the threats, customs, and laws of the country that you are visiting. One of the best resources available for information on almost every country is the U.S. State Department website, http://www.state.gov/travelandbusiness/ .

Remember:
Be Alert
Be Able to React
Maintain a Low Profile
Be Unpredictable in Your Movements – Avoid Predictable Patterns
Follow the DoD Travel Check List
Report Unusual Circumstances or Contacts to your Supervisor, SSO, and U.S. Embassy Personnel immediately, within 72 hours.

The Best Possible Defense is to Understand the Possibility of the Threat Against You – a High Priority Target!

Physical Security: Getting a SCIF Accredited

In today's post -9/11 world security is at an all time high. One can never take security lightly at any time or place. There are several types of security but one of the most important is Physical Security. Physical Security protects against all enemies, domestic and foreign, when it comes to Sensitive Compartmented Information at any level. Sensitive Compartmented Information Facility (SCIF) design must balance threats and vulnerabilities against appropriate security measures in order to reach an acceptable level of risk. If there is a need to store, use, discuss, or electronically process SCI at any level, you are required to have a SCIF. A SCIF is an accredited area, room, group of rooms or buildings or installation where SCI may be stored, used, discussed and electronically processed. The Physical Security standards for construction and protection of SCIFs are prescribed in Director of Central Intelligence Directive (DCID) 6/9 "Physical Security Standards for SCIFs." DoD SCIFs will be established according to DoD 5105.21-M-1 as well. When requesting a SCIF, there are three basic steps which must be followed to establish a DIA; Director of Administration SCIF Support Branch (DAC-2A2) accredited SCIF.

The steps are as follows:

1. The first step is submitting a Concept Approval, also known as concept validation, which is your justification for having or needing a SCIF. This request should explain your need for processing, storing or discussing SCI at any level. This is a request from you to your Major/Unified Command or Defense Agency. Before building a SCIF you need this approval. (Note) If you are unsure of who can approve your concept approval/validation request, consult with your servicing SSO, the Cognizant Security Authority (CSA) or check the concept approval point of contact listing located on the DIA JWICS or SIPRNET website. For an example of a concept approval/validation, please contact your serving SSO or SSO DIA/DAC-2A2 for an example.

2. The second step is submitting a Pre-Construction Approval /Fixed Facility Checklist (FFC). The preconstruction FFC is your blue print and the primary document in the decision making process for building and getting your SCIF accredited. DIA/DAC-2A2 will review the FFC line by line to see if you meet or exceed the requirements of DCID 6/9. SSO DIA/DAC-2A2 also has the authority to

waive requirements if you have taken adequate compensatory measures. If you establish a good rapport with SSO DIA/DAC-2A2 and ask lots of questions while filling out the preconstruction FFC, you will find that you won't have much work to do in getting your final accreditation. Once your preconstruction FFC is approved, you can start construction on your SCIF. To save yourself some valuable time and money, DO NOT start installing alarms, doors, locks, filters, etc. until you have received approval of your preconstruction FFC. Questions regarding accreditation should be forwarded to the experts accrediting your SCIF within SSO DIA/DAC-2A2.

3. The third and final step is Accreditation. This is the preconstruction checklist with all the changes requested by your accreditation authority. Submit only those pages of the preconstruction FFC that reflect changes to construction, installation of telephones, alarms, security, and other applicable modifications. Annotate your changes by placing an asterisk (*) by the page and paragraph. The following additional documents MAY be required specification sheets for Intrusion Detection Systems (IDS) component parts, UL 2050 Certification for IDS, NIST 128 bit certificate for IDS, IDS test results, SAP Co-Utilization agreements (if applicable), TSCM reports, and catastrophic failure plan prior to granting your SCIF accreditation.

In closing, after getting a SCIF accredited there are certain security measures that must be enforced on a day to day basis to ensure the protection of SCI material and to prevent security incidents/violations from happening. Always remember when you are uncertain about procedures or criteria regarding your SCIF, G-2 SSO will be there for your assistance.

Your Keys to Security

SSO
(703) 697-1577
Personnel Security
(703) 695-2758
Physical Security
(703) 697-6349
Unclassified Fax: (703) 697-3466 **DSN:** 227-3466
Secure Fax: (703) 695-6426 **DSN:** 225-6426
Customer Service Hours: 0700-1700